**MATH 587/CSCE 557: HOMEWORK 10, DUE APR 26.**

1. Suppose we want to hash a message $x$ which is made up of bytes (strings of bits of length 8). Define $f(x_1x_2x_3x_4x_5x_6x_7x_8) = x_2x_1x_4x_3x_6x_5x_8x_7$. If a message is a string of $8k$ bits, so $k$ bytes, say $m_1, m_2, ..., m_k$, compute successively $c_1 = f(m_1), c_2 = f(c_1 + m_2), c_3 = f(c_2 + m_3), ..., c_k = f(c_{k-1} + m_k)$. The hash of $m$ is then $h(m) = c_k$.

(a) Which mode of operation is this? (Electronic Codebook, Cipher Block Chaining, or Cipher Feedback).

(b) Compute the hash of 101101011101000100101101.

(c) Either find two different 24-bit messages that hash to the same value or explain why this is a good hash function.

2. Zero-knowledge proofs are where you convince someone you can do something without actually giving away the proof. For example, suppose Alice wants to convince Bob that she knows a number $x$ without Bob figuring out $x$ (this has applications e.g. in banking).

Here's how she does it. She picks two large primes $p, q$ and sets $N = pq$. She picks a number $x$ between 1 and $N$. She tells Bob $N$ and $x^2 \pmod N$ (over a public channel). If Bob could factor $N$, then he could compute $x$ and it is believed that there is no easier way to find $x$.

Alice now picks a random integer $r$ and sends Bob $x^2r^2 \pmod N$. Bob randomly sends one of two questions - "Send me $r$" or "Send me $xr \pmod N$".

(a) Show that Alice can satisfy both these requests.

(b) Show that Bob can check her answer in either case.

(c) Suppose Oscar tries to fool Bob by making up a random number $s$ and sending $s^2$ to Bob. Show that if Bob asks for $xr \pmod N$, Oscar is OK, but that if Bob asks for $r$, then Oscar is caught. Why does this mean that by playing this game several times with different $r$, Alice gives a zero-knowledge proof with high probability.

[There is an algorithm that given $r$ and $xr \pmod N$ lets you calculate $x$.]